WHAT IS CLAIMED IS:

~~Patent Claims~~

1. A method for loading input data into an algorithm when performing an authentication between electronic cash cards and a security module, where the cardholder may have a stored credit balance available to him or her, and where, for every cash transaction, the cash amount requested or input by the cardholder is debited from the cardholder's chip card with the aid of a security function, and the cash amounts are added and stored in a summing counter for cash amounts of the security module, and where for the authentication algorithm, a linear-feedback shift register is used, whose non-linear functions are cryptographically enhanced in conjunction with downstream counters, and where input data, such as a random number, a secret key, and non-secret card data, enter into this algorithm,
wherein input data are subdivided into a plurality of blocks of data, and while the blocks are loaded into the linear-feedback shift register, an additional, further feedback is introduced into the shift register following the downstream counter and is switched off following a predefined number of clock pulse steps.

2. The method as recited in Claim 1,
wherein the card data D having a secret key K are introduced as a first block, and a random number R is introduced as an additional block.

3. The method as recited in Claim 1 and 2,
wherein during the phase in which the input data are loaded, other counter contents are used than during the subsequent phase after the input data are loaded to calculate the authentication token.

4. The method as recited in Claim 1 and 2,
wherein the first downstream counter counts to 1.

5. The method as recited in Claim 1 and 2, wherein the counter and the number of clock pulses to be implemented are selected with precision so as to ensure that the authentication token is calculated based on a number of clock pulses that is fixed by other system conditions.

6. The method as recited in one of Claims 1 through 5, wherein the outputting of bits begins after all input data have been loaded.

7. The method as recited in one of Claims 1 through 6, wherein in the time between the loading of the blocks from Claim 1 and the outputting of the bits, the entire circuit continues to be pulsed for several clock pulses while the additional feedback is maintained, without input data being loaded.

8. The method as recited in one of Claims 1 through 6, wherein in the time between the loading of the blocks from Claim 1 and the outputting of the bits, the entire circuit continues to be pulsed for a certain number of clock pulses after the additional feedback is switched off, without input data being loaded.

9. A device for loading input data into an algorithm when performing an authentication using a cryptographic MAC function, made up of a linear-feedback shift register having a nonlinear "feed-forward" function, which reads off from the shift register and, using a counter, influences the output of the shift register, to which an additional counter is connected downstream, wherein the circuit, which is produced from the linear-feedback shift register and which has downstream counters to be used for the authentication algorithm, is cryptographically enhanced by an additional, disconnectable non-linear feedback.

10. The device as recited in Claim 9, wherein the additional feedback is tapped off following the first downstream counter before the latch.

11. The device as recited in Claim 9, wherein the additional feedback is read off from the latch following the first downstream counter.

12. The device as recited in Claim 9, wherein the additional feedback is read off following the second downstream counter.

13. The device as recited in Claim 9, wherein the additional feedback is generated as an XOR sum of the readouts following the first downstream counter before the latch, from the latch following the first downstream counter, and following the second downstream counter.

14. The device as recited in Claim 9, wherein the counters are subdivided or reduced.

APP A57